REMARKS

This paper amends Claims 1, 3, 4, 6, 7, 12, 14-18, 20, 21, 22, 26, 28 and 29, and cancels Claims 5 and 30-32. Claims 2, 8-11, 13, 19, 23-25, and 27 are unchanged. Claims 1-4 and 6-29 are pending. Reconsideration and allowance of the claims is respectfully requested. The amendments of Claims 3, 4, 6, 7, 12, 15, 16, 21, 22 and 29 are for clarification, and not to narrow the claim or overcome the cited references.

Discussion of Claim Objections

Claims 14-17, 20, 22 and 26 were objected to because of informalities. Applicant has amended Claims 14-17, 20, 22 and 26 to correct the informalities. For example, in Claim 14, a comma has been inserted between "key" and "which" and between "variables" and "into". These amendments are for clarification, and are not to narrow the claim or overcome the cited references.

Discussion of the Rejection of Claims under 35 U.S.C. § 112, 2nd ¶

Claims 1-32 have been rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Applicant has amended Claims 1, 3, 4, 6, 7, 12, 14, 15, 17, 18, 20, 21, 26, 28 and 29, and has canceled Claims 5 and 30 to clarify the features and to improve the intelligibility of the claims.

In Claim 1, the wording "at least one" has been amended to "a" (twice). Further, the homodyne detector is now "configured to measure the quadrature components of the states and to receive the raw key".

In Claim 3, the wording "sent and received raw data [...] are converted" has been amended to be "raw key [...] is converted". The feature is based on the wording as in Claim 1.

In Claim 4, the wording "with a high signal to noise ration" is deleted and the wording "encodes" is amended to be "is configured to encode". The amendment is supported by ¶15 and ¶ 45 of the specification. The term "several" in Claim 4 has been amended to be "a plurality of".

In Claim 6, the wording "in case of noisy quantum channels with low losses" has been deleted. The amendment is supported by ¶16 of the specification.

In Claim 7, the wording "in case of noisy quantum channels with high losses" has been deleted. The amendment is supported by ¶ 16 of the specification.

In Claim 12, the wording "typically containing several photons" has been deleted. The amendment is supported by ¶ 13 of the description.

In Claim 14, the term "the wrong one" is replaced by "the quadrature x or p that was not measured". The subject of the verb "comprising" is submitted to be "converting". Hence, the limitation now reads "the converting comprising:" (reconciliation and privacy amplification). The wording "get" is amended to be "to get".

In Claim 15, the term "which comprises the following" is amended to "the reconciliation comprising". The term "reconciliating" has been amended to be "reconciling".

In Claim 20, the term "several" has been amended to be "a plurality of".

In Claim 21, the limitation "the post-processing protocols" is amended to "post-processing protocols".

Claim 26, the term "the wrong one" is replaced by "the quadrature x or p that was not measured". Further a comma has been inserted between "key" and "in" and between "variables" and "into". The subject of the verb "comprising" is submitted to be "converting". Hence, the feature now reads "said converting comprising:" (reconciliation and privacy amplification). The wording "get" is amended to be "to get".

Claim 28 is amended to refer to the device of Claim 17. The term "are continuously modulated" is amended to be "that are modulated with a continuous distribution". The term "many" has been amended to be "a plurality of".

In Claim 29, the term "several" has been amended to be "a plurality of".

Discussion of the Rejection of Claims under 35 U.S.C. § 103(a)

Claims 1-32 have been rejected under 35 U.S.C. § 103(a) as being obvious over Nambu (U.S. Patent No. 6,801,626) in view of Ralph, "Continuous variable quantum cryptography".

Prima Facie Obviousness Requires a Teaching or Suggestion of All Claim Limitations

M.P.E.P. § 2143.03 recites that all claim limitations must be taught or suggested. To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or

suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

Analysis

Claim 1

Claim 1 has been amended to include "a sending unit comprising an encoder and configured to distribute a raw key in the quadrature components of quantum coherent states by modulating the quantum coherent states with a continuous distribution in phase and amplitude". Support for the amendment can be found in ¶12 of the application specification ("Gaussian-modulated coherent states [...] other continuous distributions may be used as well").

Amended Claim 1 now states that the phase shift and amplitude modulation of the quantum coherent states follows a *continuous distribution*, such as for example a Gaussian distribution. The present application teaches that the modulation be performed with a continuous distribution. In the present application, numbers are selected from a continuous distribution, meaning real, non-binary (and hence continuous) numbers. It follows that the raw key contains continuous data. The continuous distribution modulation allows to perform all security and error rate analysis on continuous numbers, which is faster and provides improved security compared to prior systems.

Furthermore, the conversion of the continuous raw data (i.e., the raw key) to a usable (i.e., secret) *binary* key can be deferred to after the homodyne detection, namely in a continuous reconciliation protocol (see ¶ 10 of the specification and for example Claims 3, 6 and 7), whereas in prior systems, the raw key is already binary.

Both Nambu and Ralph fail to disclose, teach or even suggest to use a continuous distribution for modulating the quantum coherent states.

Nambu fails to disclose that the quantum states are modulated in phase and amplitude. In addition, Nambu fails to disclose that the modulation be performed with a continuous distribution. In col. 7, ll. 15-28, Nambu discloses to modulate (encode) a light pulse with a random *bit* sequence supplied from a random number generator. Hence, the sequence taught by

Nambu comprises bits. Such a sequence can not be drawn from a *continuous* distribution. The protocol suggested by Nambu is hence not even a continuous variable protocol.

Ralph discloses on page 1, right column, second paragraph that "Alice generates two independent random strings of numbers and encodes one on the phase quadrature and the other on the amplitude quadrature". The encoding considered by Ralph is binary pulse code modulation in which *number strings are digitally encoded* (see Ralph, page 2, left column, second paragraph and page 2, right column, third paragraph). In direct contrast, Claim 1 recites that the modulation is performed with a *continuous* distribution, hence a modulation with continuous, real numbers, and not binary numbers.

Furthermore, Ralph suggests in the summary on page 4, right column, last paragraph that a cryptographic scheme based on coherent light is inferior to (i.e., provides much less security) than single-photon quanta schemes (see also Ralph on page 2, right column, 2nd paragraph), while a scheme based on squeezed light offers equivalent security, wherein it is essential that the coherence between the two squeezed light modes is destroyed. Hence, the person skilled in the technology is taught by Ralph to implement a quantum cryptographic system based on squeezed light which is not coherent. Ralph fails to teach, or even suggest the person skilled in the technology to implement a quantum cryptographic scheme wherein coherent states are modulated with a continuous distribution.

As stated in ¶ 10 of the specification of the present application, there is no need for such squeezed light beams. The present system and method allows to obtain an equivalent level of security by using continuous distribution modulation of coherent states. Therefore, a system is presented which is easier to implement and which allows to attain at least an equivalent level of security compared to quantum cryptographic systems of the prior art (see also ¶ 45 of the specification).

Applicant therefore respectfully submits that it is not obvious to arrive at the terms of Claim 1 by the disclosure made by Nambu in the view of Ralph.

Claim 14

Both Nambu and Ralph fail to disclose, teach or even suggest "selecting at a sender, two random numbers x_A and p_A from a Gaussian distribution of mean zero and variance $V_A N_0$, where N_0 refers to the shot-noise variance" and "sending a corresponding coherent state $|x_A+ip_A\rangle$ in the quantum channel" as recited in pertinent part in Applicant's Claim 14.

Nambu, in col. 10, ll.26-33, refers to a Gaussian distribution for the expected probability distribution of a transmitted state at "the *receiver's output*". At ll.51-57 in col. 10, Nambu refers to the observation (hence necessarily at a receiver) of Gaussian distribution of the transmitted signal. The disclosure by Nambu is not at all linked to the features of Claim 14.

The use of numbers from a Gaussian distribution for encoding into a quantum channel allows to make the security of the cryptographic protocol easier to analyze compared to the prior art (see ¶¶ 44-45 of the specification).

Hence, Claim 14 is respectfully submitted not to be obvious in the view of Nambu and Ralph.

Claim 17

In Claim 17, the term "continuously modulate" has been amended to be "modulate with a continuous distribution". The amendment is in accordance with the amendment to Claim 1. Claim 17 is respectfully submitted not to be obvious in view of Nambu and Ralph.

Claim 20

In Claim 20, the term "and is continuously modulated" has been amended to be "each pulse being modulated with a continuous distribution". The amendment is in accordance with the amendment to Claim 1 and to Claim 17. Claim 20 is respectfully submitted not to be obvious in view of Nambu and Ralph.

Dependent Claims

Applicant respectfully submits that Applicant does not necessarily agree with the characterization and assessments of the dependent claims made by the Examiner, and Applicant believes that each claim is patentable on its own merits. Claims 2-4, 6-13, 15-16, 18-19 and 21-29 are dependent either directly or indirectly on the above-discussed independent claims. Applicant respectfully submits that pursuant to 35 U.S.C. § 112, ¶4, the dependent claims

incorporate by reference all the limitations of the claim to which they refer and include their own patentable features, and are therefore in condition for allowance. Therefore, Applicant respectfully requests the withdrawal of all claim rejections and prompt allowance of the claims.

Conclusion

In view of the foregoing remarks, Applicant respectfully submits that the claims of the above-identified application are in condition for allowance. However, if the Examiner finds any impediment to allowing all claims that can be resolved by telephone, the Examiner is respectfully requested to call the undersigned.

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: December 5, 2007

By: Raimond Salenieks

Raimond J. Salenieks
Registration No. 37,924
Agent of Record
Customer No. 20,995
(619) 235-8550

4607744 / 120307